UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/599,230	09/22/2006	Karl Asperger	071308.0761	6068

31625 7590 08/17/2009

BAKER BOTTS L.L.P.
PATENT DEPARTMENT
98 SAN JACINTO BLVD., SUITE 1500
AUSTIN, TX 78701-4039

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
08/17/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/599,230	ASPERGER ET AL.	
	Examiner	Art Unit	
	JASON LEE	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/22/06, 05/02/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 09/22/2006, 05/02/2008 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Drawings

3. The drawings filed on 09/22/2006 are accepted.

Priority

4. This application is related to and claimed the benefits of Germany Patent application No.10 2004 014 435.4 filed 03/24/2004.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-4, 6-8, 10-1, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamauchi et al (US 2002/0040420 A1), hereinafter Yamauchi, in view of Anderson et al (US 2003/0084336 A1) hereinafter Anderson.

Regarding to claim 1:

Yamauchi discloses an integrated circuit **(e.g. see Yamauchi [0309] " FIG. 36 is a conceptual block diagram representing a configuration when the semiconductor**

integrated circuit device 1 operating in the block mode is applied to a system in which a cache memory 96 exist. ") comprising function modules, wherein the function modules comprise a central processing unit designed to process data and to execute programs **(e.g. see Yamauchi [0290] "The microcomputer 90 includes: a CPU core 94, a memory controller 98; and an external bus interface circuit 100, wherein the constituents are connected to each other by an internal bus 102. The CPU core 94 is connected to a flash memory 106 in which data to be enciphered or deciphered is stored through a serial interface 104. ")** , and a cache memory **(see Yamauchi [0296] "The microcomputer 90 includes: a CPU core 94; a cache memory 96; a memory controller 98; and an external bus interface circuit 100, wherein the constituents are connected to each other by an internal bus 102.")** , wherein the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules comprise a security sensor system by means of which at least one operating parameter of the integrated circuit is monitored, wherein, as operating parameters, the state of a protective layer on the integrated circuit is monitored. Yamauchi discloses the CPU and cache memory as above, but does not disclose wherein the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules comprise a security sensor system by means of which at least one operating parameter of the integrated circuit is monitored, wherein, as operating parameters, the state of a protective layer on the integrated circuit is monitored.

However, Anderson discloses the function modules (e.g. page 4 of specification [0012] "frequency of clock, operating voltage and operating temperature sensors for protective layers) comprise an encryption unit designed to encrypt and decrypt data **(see Anderson [0007] "The techniques in our invention apply without loss of generality to security processors which are not microprocessors, such as dedicated encryption chips and modules which contain more than one chip (e.g., separate processor, cryptographic chip and RAM in a single package). ")** and the function modules comprise a security sensor system by means of which at least one operating parameter of the integrated circuit is monitored, wherein, as operating parameters, the state of a protective layer on the integrated circuit is monitored. **(see Anderson [0008] "Our invention is adapted from dual-rail encoded asynchronous logic because in this technology, the power consumed can be made substantially independent of the data being processed, and by the choice of suitable design rules, which should be clear to those skilled in the art, the design can be made resistant to single-transistor and single-wire faults. Furthermore, such circuits are already known to be highly resilient to variations in the applied power supply voltage. In our invention, alarms resulting from environmental sensors or from the activation of other protective mechanisms can be propagated rapidly through the chip using many independent paths.") and [0014] "Other sensors are outside the scope of this patent but may typically be designed to detect out-of-bounds environmental parameters such as over- and under-voltage and low temperature.") and [0037] "Clock Frequency Modulation for Secure Microprocessors")**

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Yamauchi to include function modules comprise a security sensor system by means of which at least one operating parameter of the integrated circuit is monitored as taught by Anderson because they are analogous in the secure microprocessor and one of ordinary skill in the art would have been motivated to incorporate the teaching of Anderson in Yamauchi of using the security sensor to propagate alarms quickly in the event of an attack being detected and therefore achieve robustness and fragility with existing silicon technology. **(see Anderson [0006])**

As for claim 20:

Yamauchi discloses an integrated circuit **(see Yamauchi [0309] " FIG. 36 is a conceptual block diagram representing a configuration when the semiconductor integrated circuit device 1 operating in the block mode is applied to a system in which a cache memory 96 exist. ")** comprising function modules, wherein the function modules comprise a central processing unit designed to process data and to execute programs **(see Yamauchi [0290] "The microcomputer 90 includes: a CPU core)**, and a cache memory**(see Yamauchi [0296] "The microcomputer 90 includes: a CPU core 94; a cache memory 96)**, wherein the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules comprise a security sensor system by means of which at least one operating parameter of the integrated circuit is monitored, wherein, as operating parameters, the state of a protective layer on the integrated circuit is monitored, wherein the function modules comprise a random-

number generator and a first memory in which cryptological keys are stored, and wherein cryptological keys which are stored in the first memory are generated by means of the random-number generator. **(see Yamauchi [0599] " A secrete key cryptosystem which can be used is notified and a random number and a current time point is sent to the host side . [0600] 6) The host side determines a secret key cryptosystem and notifies the client side of which secrete key cryptosystem is adopted and obtains the random number and the current time point . [0601] The client generates random numbers serving as a base of a secret key. [0602] The random numbers generated are enciphered with the public key of the server and thereafter sent to the server .)**

Yamauchi discloses the CPU and cache memory, Random-number generator as above, but does not disclose the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules comprise a security sensor system by means of which at least one operating parameter of the integrated circuit is monitored, wherein, as operating parameters, the state of a protective layer on the integrated circuit is monitored.

However, Anderson discloses the function modules comprise an encryption unit designed to encrypt and decrypt data and the function modules comprise a security sensor system by means of which at least one operating parameter of the integrated circuit is monitored, wherein, as operating parameters, the state of a protective layer on the integrated circuit is monitored**(see Anderson [0008] "Our invention is adapted from dual-rail encoded asynchronous logic because in this technology, the power**

consumed can be made substantially independent of the data being processed, and by the choice of suitable design rules, which should be clear to those skilled in the art, the design can be made resistant to single-transistor and single-wire faults. Furthermore, such circuits are already known to be highly resilient to variations in the applied power supply voltage. In our invention, alarms resulting from environmental sensors or from the activation of other protective mechanisms can be propagated rapidly through the chip using many independent paths.") and [0014] "Other sensors are outside the scope of this patent but may typically be designed to detect out-of-bounds environmental parameters such as over- and under-voltage and low temperature.") and [0037] "Clock Frequency Modulation for Secure Microprocessors")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Yamauchi to include function modules comprise a security sensor system by means of which at least one operating parameter of the integrated circuit is monitored as taught by Anderson because they are analogous in the secure microprocessor and one of ordinary skill in the art would have been motivated to incorporate the teaching of Anderson in Yamauchi of using the security sensor to propagate alarms quickly in the event of an attack being detected and therefore achieve robustness and fragility with existing silicon technology. **(see Anderson [0006])**

As for claim 2:

The combination of Yamauchi and Anderson teaches the integrated circuit as according to claim 1, wherein the function modules comprise a random-number generator. **(see Yamauchi [0599] " A secrete key cryptosystem which can be used is notified and a random number and a current time point is sent to the host side . [0600] 6) The host side determines a secret key cryptosystem and notifies the client side of which secrete key cryptosystem is adopted and obtains the random number and the current time point . [0601] The client generates random numbers serving as a base of a secret key. [0602] The random numbers generated are enciphered with the public key of the server and thereafter sent to the server .)**

As for claim 3:

The combination of Yamauchi and Anderson discloses the integrated circuit as according to claim 1, wherein function modules comprise a first memory in which cryptological keys are stored. **(see Yamauchi [0470] and FIG 54 " At Y addresses #10 to #13, stored is a first key of 64 bits in length, and at Y address #14 to #17, stored is a second key of 64 bits in length.")**

As for claim 4:

The combination of Yamauchi and Anderson discloses the integrated circuit as according to claim 1, wherein cryptological keys which are stored in the first memory are generated by means of the random-number generator. **(see Yamauchi [0598]-[0602])**

As for claim 6:

The combination of Yamauchi and Anderson discloses the integrated circuit as according to claim 1, wherein operating parameters to be monitored additionally is the

clock frequency of the real-time clock **(see Anderson [0037] "Clock Frequency Modulation for Secure Microprocessors,")** and/or an operating temperature at a point in the integrated circuit and/or an operating voltage of the integrated circuit. **(see Anderson [0014] "Other sensors are outside the scope of this patent but may typically be designed to detect out-of-bounds environmental parameters such as over- and under-voltage and low temperature.")**

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Yamauchi to include operating parameters such as clock frequency and/or operating voltage of the integrated circuit as taught by Anderson because they are analogous in the secure microprocessor and one of ordinary skill in the art would have been motivated to incorporate the teaching of Anderson in Yamauchi of using the security sensor to propagate alarms quickly in the event of an attack being detected and therefore achieve robustness and fragility with existing silicon technology.

As for claim 7:

The combination of Yamauchi and Anderson discloses the integrated circuit as according to claim 1, wherein at least one limit value is predetermined for the operating parameter to be monitored, the operating parameter is measured and compared with the limit value and when the result exceeds or drops below the limit value, the content of the first memory is deleted. **(see Anderson [0014]" One sensor in our invention is based on an instruction counter; the processor software can check that the expected number of instructions have been executed and alarm if this is riot the**

case (as might happen, for example, under destructive probing attack). In the single circuit implementing the instruction by which this alarm is executed, we depart from the quad-coded logic rules described herein so that an alarm hardware state may be generated from a non-alarm hardware state. Other sensors are outside the scope of this patent but may typically be designed to detect out-of-bounds environmental parameters such as over- and under-voltage and low temperature.") and [0015]" Once an alarm signal has been injected into the data-path it obliterates the data in the pipeline since any dyadic function of a valid logic level with an alarm signal will result in an alarm signal.")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Yamauchi to include operating parameter measure as taught by Anderson because they are analogous in the secure microprocessor and one of ordinary skill in the art would have been motivated to incorporate the teaching of Anderson in Yamauchi of using operating measure for sensor to propagate alarms quickly in the event of an attack being detected and therefore achieve robustness and fragility with existing silicon technology.

As for claim 8:

The combination of Yamauchi and Anderson discloses the integrated circuit as according to claim 1, wherein it is arranged in a package and has terminal contacts brought out of the package. **(see Anderson [0007]" The techniques in our invention apply without loss of generality to security processors which are not microprocessors, such as dedicated encryption chips and modules which**

contain more than one chip (e.g., separate processor, cryptographic chip and RAM in a single package)." And [0003] "an attack using power analysis can be devised which will work against other cards of the same type without the need to depackage them. A particularly grave threat is that such an attack might be implemented in a seemingly innocuous terminal, in which members of the public might insert smartcards issued by a bank or government in order to obtain some low cost service.")

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Yamauchi to include package as taught by Anderson because they are analogous in the secure microprocessor and one of ordinary skill in the art would have been motivated to incorporate the teaching of Anderson in Yamauchi of using package for security sensor to propagate alarms quickly in the event of an attack being detected and therefore achieve robustness and fragility with existing silicon technology.

As for claim 10:

The combination of Yamauchi and Anderson discloses the integrated circuit as according to claim 1, wherein the function modules comprise an integrated voltage regulator which regulates an operating voltage. **(see Yamauchi [0743] "a configuration is adopted in which a level of the internal power source voltage is variable according to a cycle of an input clock." And [0744] "By adopting such a configuration, in a system that is allowed to be operated at a low speed, an internal voltage level is altered such that a speed of an internal operation of the**

DRAM section is reduced in conformity with a system speed, whereby reduction in power consumption can be achieved at a given clock frequency")

As for claim 11:

The combination of Yamauchi and Anderson discloses the integrated circuit as according to claim 1, wherein it is constructed as semiconductor chip. **(see Anderson [0005]" Existing defensive technology includes randomized internal clock generators to deny precise timing information to an attacker [14], incorporating a number of oscillators and/or noise generators to provide masking signals, physical chip coatings to make probing more difficult, sensor grids in the top metal layer of the chip which may be broken during probing attacks and activate alarms")**

It would have been obvious for one of the ordinary skill in the art at the time of the invention was made to modify the invention of Yamauchi to include chip as taught by Anderson because they are analogous in the secure microprocessor and one of ordinary skill in the art would have been motivated to incorporate the teaching of Anderson in Yamauchi of using chip for security sensor to propagate alarms quickly in the event of an attack being detected and therefore achieve robustness and fragility with existing silicon technology.

7. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamauchi and Anderson as applied to claims 1 above, further in view of Nakajima et al (US 2004/0106239 A1), hereinafter Nakajima.

As for claim 5:

The combination of Yamauchi and Anderson teaches the integrated circuit according to claim 1. neither Yamauchi nor Anderson disclose wherein function modules comprise a real-time clock.

However, Nakajima discloses wherein function modules comprise a real-time clock. **(see Nakajima [0098] "circuitry 510 including a real-time clock, a serial interface, and a timer, a clock control circuit 511, a cache controller 512, and a bus controller 513 are formed on the dielectric film.")**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teaching of Nakajima within the combination integrated circuit of Yamauchi and Anderson because they are analogous in the secure microprocessor using real-time clock. One of the ordinary skill in the art would have been motivated to incorporate the teaching of real-time clock to provide benefit for real-time information for the security sensor in the event of an attack being detected and therefore achieve robustness and fragility with existing silicon technology.

8. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamauchi and Anderson as applied to claims 1 above, further in view of Fricke et al (US 6,711,045 B2), hereinafter Fricke.

As for claim 9:

The combination of Yamauchi and Anderson teaches the integrated circuit according to claim 1, neither Yamauchi nor Anderson disclose wherein individual function modules have an essentially planar extent and are arranged adjacently to one another in the area of the normal to the surface.

However, Fricke discloses individual function modules have an essentially planar extent and are arranged adjacently to one another in the area of the normal to the surface. **(see Fricke column 4 lines 43-50 " FIGS. 3 and 4 schematically depict an embodiment of a memory cell that includes a memory storage element 23 disposed on a first conductor 33. A control element 25 is disposed on a second conductor 35 that is laterally or transversely adjacent to first conductor 33. Memory storage element 23 and control element 25 are thus horizontally, transversely, or laterally separated and each can have a generally horizontal planar extent.")**

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of Fricke to include the planar extent because they are analogous in the secure microprocessor and one of the ordinary skill in the art would recognize the benefit of this so to achieve robustness and fragility with existing silicon technology.

9. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamauchi and Anderson as applied to claims 11 above, further in view of Khoury (US 2001/0053565 A1), hereinafter Khoury.

As for claim 12:

The combination of Yamauchi and Anderson teaches the integrated circuit according to claim 11, but does not disclose wherein semiconductor structures of the individual function modules are intermeshed in the manner of a puzzle in order to avoid individual function modules from being recognizable.

However, Khoury discloses wherein semiconductor structures of the individual function modules are intermeshed in the manner of a puzzle in order to avoid individual function modules from being recognizable. **(see Khoury [0033]" It should be noted that other shapes are possible for interlocking edges, such as dovetail-channel connections, or "puzzle style" edges so long as the interlocking edges have shapes that intermesh to allow for one IC module to positively lock/mate with a second IC module to form a structural connection. In addition, the layers for these shapes may or may not extend through the entire edge of the substrate so long as this structural connection is formed. ")**

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of Khoury to include the individual function modules are intermeshed in the manner of a puzzle because they are analogous in the secure microprocessor and one of the ordinary skill in the art would recognize the benefit of this "puzzle style" and avoid the copy-attempt for the chip protection.

10. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamauchi and Anderson as applied to claims 11 above, further in view of Anthony et al (US 2003/0206388 A9), hereinafter Anthony.

As for claim 13:

The combination of Yamauchi and Anderson teaches the integrated circuit according to claim 11, but does not disclose wherein an active protective layer which consists of at least one elongated electrical line which extends along the surface of the die,

particularly in mutually parallel tracks section by section, is applied directly to the die of the semiconductor chip.

However, Anthony discloses wherein an active protective layer which consists of at least one elongated electrical line which extends along the surface of the die, particularly in mutually parallel tracks section by section, is applied directly to the die of the semiconductor chip. **(see Anthony [0101] "To provide electrical connections between electrode pathway 16A and 16B and their respective conductive band 40A and 40B while at the same time maintaining electrical isolation between other portions of multi-functional energy conditioner 10, each electrode pathway 16 is elongated and positioned such that the elongated portion of electrode pathway 16A is directed opposite of the direction electrode pathway 16B is directed. The elongated portions of electrode pathways 16 also extend beyond the distance in which the plurality of common conductive pathways common conductive pathways 14 extend with the additional distance isolated from outer edge conductive bands 40A and 40B by additional material 28.") and [0151]" Interposer 60 is also shown connected to an integrated circuit die 4100. The integrated circuit die 4100 is also shown with protective glob coating or encapsulment material 6212 just above the die surface.")**

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of Anthony to include elongated electrical line which extends along the surface of the die because they are analogous in the secure microprocessor and one of the ordinary skill

in the art would recognize the benefit of this elongated electrical line which extends along the surface of the die and provide the protective layer for the semiconductor chip.

11. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yamauchi and Anderson as applied to claims 11 above, further in view of Huttunen (US 2003/0147267 A1), hereinafter Huttunen.

As for claim 14:

The combination of Yamauchi and Anderson teaches an arrangement comprising an integrated circuit as claimed claim 1, but does not disclose wherein the integrated circuit is connected by means of a data bus to a second memory in which data are stored encrypted, wherein the second memory has memory cells which in each case have a memory address and each memory cell can be addressed directly in reading or writing manner.

However, Huttunen discloses wherein the integrated circuit is connected by means of a data bus to a second memory in which data are stored encrypted, wherein the second memory has memory cells which in each case have a memory address and each memory cell can be addressed directly in reading or writing manner. **(see Huttunen [0041] " The RAM 5 is arranged to store both program files and user data. Stored in the RAM 5 (or possibly the ROM 4) is program code for encrypting and decrypting data, typically user data files such as text files, images, contacts, spreadsheets, etc, and which is run by the microprocessor 3. The program has two modes of operation, a first encryption and decryption mode and a second encryption only mode. The user is asked to select one of these modes when the**

device is first turned on. The user may also toggle between the two modes when the device is in use. In either event, when the user wishes to use the first mode, he or she is asked to enter a passphrase. This passphrase is not required when the user selects the second mode. ")

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of Huttunen to include RAM for storing encrypted data because they are analogous in the secure microprocessor and one of the ordinary skill in the art would recognize the benefit of this RAM and provide the protective layer for the semiconductor chip.

12. Claim 15 -19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamauchi and Anderson as applied to claims 14 above, further in view of Kean (US 2001/0015919 A1), hereinafter Kean.

As for claim 15:

The combination of Yamauchi and Anderson teaches an arrangement comprising an integrated circuit as claimed claim 14, but does not wherein the second memory is volatile and is connected to a battery so that the voltage supply is maintained when another power supply is lacking.

However, Kean discloses wherein the second memory is volatile and is connected to a battery so that the voltage supply is maintained when another power supply is lacking. **(see Kean [0007] "Some users of SRAM FPGAs have implemented a battery back up system which keeps the FPGA powered on in order to preserve its configuration memory contents even when the system containing the FPGA is**

powered off. The FPGA bitstream is loaded before the equipment containing it is shipped to the end user preventing unauthorized access to the bitstream information. Present day FPGAs have a relatively high power consumption even when the user logic is not operating: which limits the life span of the battery back up. If power is lost for even a fraction of a second the system the FPGA control memory will no longer be valid and the system will cease to function.") and [0021] "A battery-backed on-chip memory stores the cryptographic key. There is an on-chip triple-DES encryption circuit. And, there is an interface to an external nonvolatile memory for storing encrypted configuration data.")

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of Kean to include battery for power supply because they are analogous in the secure microprocessor and one of the ordinary skill in the art would recognize the benefit of this battery for supply for backup and provide the protective layer for the semiconductor chip.

As for claim 16:

The combination of Yamauchi and Anderson teaches an arrangement comprising an integrated circuit as claimed claim 1, but does not disclose wherein the integrated circuit is connected by means of a data bus to a non-volatile third memory in which data or program code are stored encrypted.

However, Kean discloses wherein the integrated circuit is connected by means of a data bus to a non-volatile third memory in which data or program code are stored encrypted.

(see Kean [0022] "configuring an FPGA including loading key information into an on-chip battery-backed register. An initial configuration is loaded through a JTAG interface. An encrypted version of the configuration is stored in an external nonvolatile memory.")

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of Kean to include means of a data bus to a non-volatile because they are analogous in the secure microprocessor and one of the ordinary skill in the art would recognize the benefit of this means of a data bus to a non-volatile and provide the program code stored encrypted for the semiconductor chip.

As for claim 17:

The combination of Yamauchi and Anderson teaches an arrangement comprising an integrated circuit as claimed claim 1, but does not disclose wherein the security sensor system is connected to a battery so that the voltage supply is maintained if another power supply is lacking.

However, Kean discloses the security sensor system is connected to a battery so that the voltage supply is maintained if another power supply is lacking. **(see Kean [0021] "A battery-backed on-chip memory stores the cryptographic key. There is an on-chip triple-DES encryption circuit. And, there is an interface to an external nonvolatile memory for storing encrypted configuration data.")**

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of

Kean to include battery for security sensor because they are analogous in the secure microprocessor and one of the ordinary skill in the art would recognize the benefit of this battery for security sensor and provide the protective layer for the semiconductor chip.

As for claim 18:

The combination of Yamauchi and Anderson teaches an arrangement comprising an integrated circuit as claimed claim 1, but does not disclose wherein the security sensor system is connected to an auxiliary power source, integrated in the package, which provides the power for deleting the first memory.

However, Kean discloses wherein the security sensor system is connected to an auxiliary power source, integrated in the package, which provides the power for deleting the first memory. **(see Kean [0023] "A decryption circuit receives and decrypts a stream of encrypted configuration data using the security key. The decryption circuit also generates decrypted configuration data for configuring the static random access memory cells. When power is removed from the first positive supply input pin, the configuration of the static random access memory cells is erased, while the security key stored in the ID register is maintained by the external backup battery. In a specific embodiment, the external backup battery only supplies power to the ID register. In a implementation, the decryption circuit decrypts the stream of encrypted configuration data using a triple-DES algorithm. There may be a random number generator circuit to generate the security key.")**

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of

Kean to include an auxiliary power source (e.g. external backup battery) because they are analogous in the secure microprocessor and one of the ordinary skill in the art would recognize the benefit of this auxiliary power source and provide the protective layer for the semiconductor chip.

As for claim 19:

The combination of Yamauchi and Anderson teaches an arrangement comprising an integrated circuit as claimed claim 16, but does not disclose wherein the third memory is a Flash memory or ROM.

However, Kean discloses wherein the third memory is a Flash memory or ROM. **(see Kean [0018]" The nonvolatile storage device may be a serial EPROM or serial EEPROM. The nonvolatile storage device may be a Flash memory.")**

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Yamauchi with the teaching of Kean to include a Flash memory or ROM because they are analogous in the secure microprocessor and one of the ordinary skill in the art would recognize the benefit of this a Flash memory or ROM and provide the protective layer for the semiconductor chip.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JASON LEE/
Examiner, Art Unit 2438

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2438
August 12, 2009